

Quadrant™ Leader for Endpoint Protection Again.

CrowdStrike®

An Endpoint Protection Leader

OPEN >

Expert Insights & Resources

Expert Commentary

Cyber Threats & Vulnerabilities

Understanding and Responding to Distributed Denial-of-Service Attacks

By **Tyler Farrar**, CISO at Exabeam



Sometimes the best advice is free advice. Especially in cybersecurity, where understanding the ‘why’ behind attacks can be as crucial as defending against them. Recently, CISA, the FBI, and MS-ISAC have highlighted Distributed Denial-of-Service (DDoS) attacks, not just as random disruptions but as strategically employed tools. These attacks are often used for economic gain or as distractions to divert attention from more sinister activities. Recognizing this, the issued guidelines urge organizations to bolster their defense mechanisms. By emphasizing the importance of risk assessments, network monitoring, and incident response planning, this advice lays the groundwork for a robust cybersecurity strategy that evolves as quickly as the threats themselves.

Building on these recommendations, organizations must advance towards integrating AI-driven predictive models that are finely attuned to the shifting dynamics of DDoS attacks. As the digital landscape transforms with widespread adoption of shared cloud services and increased reliance on interconnected supply chains, the attack surface becomes more complex, often extending down to the microservice layer. This nuanced threat landscape requires detection capabilities that can preemptively identify and mitigate attacks before they exploit these hidden dependencies. AI models offer this level of sophistication by analyzing patterns that predict where vulnerabilities may emerge as businesses evolve towards digital transformation and adopt everything-as-code practices.

CROWDSTRIKE

8 Things Your Next SIEM Must Do

Unify the SOC and stop breaches faster

Download eBook

Moreover, while the emphasis on collaboration and sharing best practices is crucial, it often encounters significant cultural and procedural hurdles. Legal constraints and a predominant focus among Chief Information Security Officers (CISOs) on indicators of compromise (IOCs) rather than deeper knowledge sharing can stifle this necessary exchange. To counteract these barriers, CISOs must demand the explicit right to share information as a non-negotiable term of their employment contracts. This ensures that

the buck stops with them—not just as a participant but as a decisive leader in their field. CISOs should also use their authority to shape the conversation during interviews, making clear that their ability to share and act on information is pivotal to their role.

At the board level, steering committees should implement mandates that structure how information on cyber threats is shared across organizations and industries. These steps would not only enhance collective resilience against DDoS attacks but also firmly establish the CISO as a central figure in the network of defense, endowed with the authority to make critical decisions that protect the organization.

Remember, the journey toward cybersecurity resilience is ongoing. By embracing innovative technologies, fostering open communication, and continually refining response strategies, organizations can not only defend against DDoS attacks but also strengthen their overall cybersecurity posture.

#

About the author

Tyler Farrar is the Chief Information Security Officer (CISO) at [Exabeam](#), where he is responsible for protecting Exabeam – its employees, customers, and data assets – against present and future digital threats. Farrar also leads efforts in supporting current and prospective customers’ move to the Exabeam cloud-native New-Scale SIEM and security operations platform by helping to address cloud security compliance barriers. With more than 15 years of broad and diverse technical experience, Farrar is recognized as a business-focused and results-oriented leader with a proven record of advancing organizational security programs.

A former Naval Officer, Farrar managed multiple projects and cyber operations for a multimillion-dollar U.S. Department of Defense program. He holds an MBA from the University of Maryland and a Bachelor of Science in Aerospace Engineering from the United States Naval Academy. He also holds a variety of technical and professional certifications, including the Certified Information Systems Security Professional (CISSP) certification.

Ad

CrowdStrike®

See Why CrowdStrike Was Named a Leader In The 2023 Gartner® Magic Quadrant™ - 4X Running

OPEN >>

TAGS

Exabeam

Denial of Service attacks

DDoS



Jane Devry

RELATED ARTICLES

MORE FROM AUTHOR

Cyber Threats & Vulnerabilities

Enhancing Cyber Resilience in Banking: Leveraging Live Patching to Combat Rising Threats



Cyber Threats & Vulnerabilities

Securing Trust: How to Partner With Customers to Build World-Class Cybersecurity Solutions

Cyber Threats & Vulnerabilities

Breaking Down the WebTPA Data Breach: Expert Analysis and Perspectives

EDITOR PICKS

Enhancing Cyber Resilience in Banking: Leveraging Live Patching to Combat Rising...

Cyber Threats & Vulnerabilities

Securing Trust: How to Partner With Customers to Build World-Class Cybersecurity...

Cyber Threats & Vulnerabilities

Breaking Down the WebTPA Data Breach: Expert Analysis and Perspectives

Cyber Threats & Vulnerabilities

POPULAR POSTS

List of Countries which are most vulnerable to Cyber Attacks

Vulnerability

Top 5 Cloud Security related Data Breaches!

Cloud Security

Top 5 PCI Compliance Mistakes and How to Avoid Them

How-To Guide

RECENT POSTS

Securing Cloud Environments: Safeguarding Against Cyber Threats

Cloud Security

Fake Antivirus websites now delivering malware

Malware

Microsoft to roll out AI powered PCs concerningly in coming years

Data privacy

ABOUT US

Cybersecurity Insiders is your comprehensive source for everything related to cybersecurity - connecting people, opportunities, and ideas.

Contact us: info@cybersecurity-insiders.com

FOLLOW US

